ソリューションノート

AMAZON ROUTE 53 と INFOBLOX を使用したハイブリッドクラウド展開のためのシームレスな制御とセキュリティ

まとめ

Amazon Route 53 DNS サービスは、純粋な Amazon Web Services (AWS) 環境以外では限定的なサポートを提供します。

サポートの制限により、企業はエンタープライズキャンパスネットワークやハイブリッドクラウドを含む企業全体に対応する DNS、DHCP、IP アドレス管理 (3 つを総称してDDIと呼ぶ) の単一統合ソリューションを Route 53 だけでは作成できないことになります。Route 53 は AWS の仮想プライベートクラウド (VPC) のみに特化しているため、AWS 以外のクラウドプラットフォームで使用する際には接続性、可視性、セキュリティが制限されます。

Infoblox の業界をリードする DDI プラットフォームは AWS 及び Amazon Route 53 と統合可能であり、AWS とハイブリッドクラウド展開用の商用、エンタープライズ、サービスプロバイダーグレードの統合ソリューションとなります。Infoblox と Amazon Route 53 の統合は、企業の IT チームとクラウドチームの間のギャップを埋めます。オンプレミス、プライベートクラウド、AWS パブリッククラウドの展開を管理するための単一のコントロールプレーンを提供すると同時に、これらの展開のセキュリティを強化することで、複雑さを軽減しながら、最適なセキュリティレベルを確保します。このソリューションは、AWS への拡張を進め、DNS に Amazon Route 53 を利用している現在および将来の Infoblox のお客様のニーズを満たします。

可視性、自動化、一貫性の欠如が AMAZON ROUTE 53 の展開上の課題に

Amazon Route 53 は、AWS VPC 内でプライベート DNS 機能を提供します。ただし、ハイブリッドクラウドを使用する企業は、Amazon Route 53 の使用時に、以下のような運用上の課題に直面します。

- **DNS の制限:** DNS の解決またはクエリへの応答は AWS ネットワーク内で隔離されているため、特定の AWS プライベートホストゾーンの外部で通信が必要な場合に問題が生じます。IT チームは多くの場合、この問題を解決するために、複数の BIND サーバーを立ち上げて、隔離された AWS ゾーンの外部に DNS トラフィックを通過させます。この解決策には、複雑さが増し、異なる DNS 展開間の一貫性が欠如するという欠点があります。
- **IPAM の欠如:** AWS は IP アドレス管理 (IPAM) ソリューションを提供しておらず、仮想インスタンスの可視性が制限されることが多いため、日常の管理に悪影響が及び、監査やコンプライアンスの所要時間が増えます。

AMAZON ROUTE 53 を使用して統合された DNS および IPAM ソリューションを構築する

Infoblox DDI for AWS は Amazon Route 53 DNS サービスと統合し、AWS およびハイブリッドクラウドの展開全体にわたる集中コンソールとして、可視性、一貫した管理、セキュリティを実現します。この統合ソリューションにより、Amazon Route 53 プライベートホストゾーンに限定されることなく、AWS 以外でも信頼性の高いハイブリッドクラウドの展開が可能になります。

- **ハイブリッドクラウドの可視性の欠如:** ハイブリッドクラウド全体に一貫して対応する DNS および IPAM ソリューションがない場合、企業の IT 部門は DNS および IP アドレスデータにアクセスするために複数のツールを使用せざるを得ません。こうした可視性の欠如は、トラブルシューティングの時間を長引かせ、ネットワーク計画の実行能力を低下させ、セキュリティリスクを増大させます。また、企業全体での DNS および IP アドレススペースの管理に多数の矛盾が生じます。
- **DNS セキュリティが限定的:** Route 53 は、AWS およびハイブリッドクラウドの展開に対して、高度な脅威検出機能を提供しますが DNS セキュリティは限定的です。DNS トンネリングを利用したデータ流出や DNS を利用したマルウェアは、IT ネットワークの麻痺を起こしかねない一般的な脅威です。

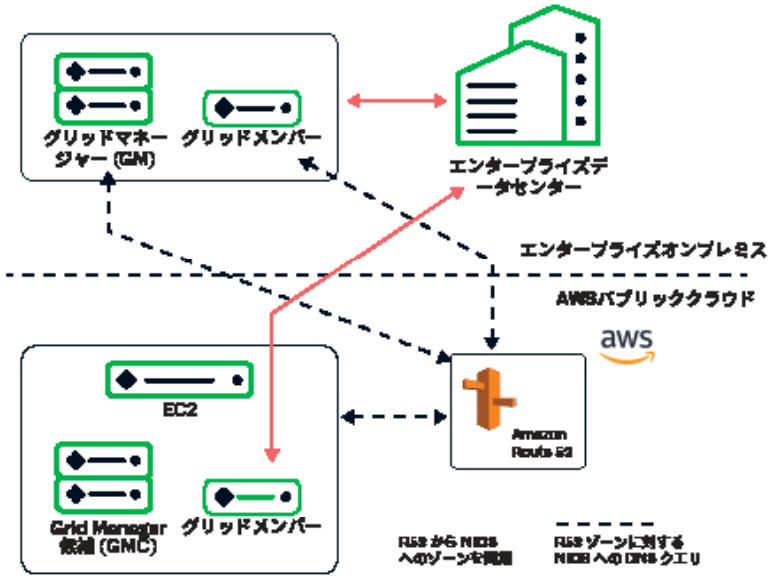


図1: ハイブリッドクラウド全体を統合管理

AWS とハイブリッド展開全体のコンテキストを伴う可視性を向上

今日のハイブリッドマルチクラウド環境では、ネットワークの可視性が非常に重要です。Route 53 は AWS の仮想リソースに特化しているため、可視性はこうしたパブリッククラウドインスタンスに限定されます。Infoblox と AWS のソリューションは、VPC と EC2 インスタンスの自動検出、強化された可視性と追跡を単一のプラットフォームで提供し、パブリッククラウド資産を共通の DNS と IPアドレス管理下に容易に取り込むことができます。Infoblox は、インスタンスが破棄された後のレコードの作成とクリーンアップを簡素化します。選択的クラスレスドメイン間ルーティング (CIDR またはプライベート IP) vDiscovery を使用してネットワークリソースを検出し、含めたり除外したりして、AWS での IP アドレスの効率的な配布を確保します。

Amazon Route 53 で複数のアカウントを管理および同期する必要があるチームにとって、Infoblox は、各アカウントでの vNIOS メンバーの展開を排除し、すべての Route 53 ホストゾーンを Grid に同期することで、時間と AWS の使用料金を大幅に節約します。vDiscovery は、複数の AWS リージョンとアカウントにわたる複数の検出タスクを 1 つの検出ジョブに集約します。また、アカウントフィルターを保持することで、データを失うことなく既存の vDiscovery ジョブのリージョン選択と移行が可能になり、ユーザーエクスペリエンス、ワークロード効率、管理者の制御が向上します。

Infoblox は、連邦政府およびその他の政府機関のお客様に、複数の AWS GovCloud リージョンとアカウント向けの Route 53 同期サポートと vDiscovery を提供することで、可視性と制御をさらに充実させます。その結果、可用性と拡張性に優れた DNS が提供され、ユーザーのリクエストを AWS インターネットアプリケーションに接続し、カスタマイズされたルーティングポリシーによって遅延を低減します。

ITチームは、コンプライアンス、運用、エグゼクティブレポートのために、AWSとAWS以外のパラメータを単一のコントロールプレーンで一貫して表示することで、DNSおよびIPアドレス情報の監査に必要な時間を大幅に短縮できます。

優れた可用性、稼働時間、耐久性

NIOS を使用すると、クラウドプラットフォーム (CP) アプライアンスを実行している顧客は、高い可用性 (HA) と稼働時間のために 2 つの NIOS アプライアンスを構成できます。HA は、ユーザーがどれだけ信頼性高くシステムにアクセスできるか、および計画的なメンテナンスや予期しないダウンタイムの影響を受けるかどうかを測定するものです。アップタイムは、システムが稼働している時間を測定します。NIOS を使用することで、管理者は両方を実現することができ、特にミッションクリティカルアプリケーションやワークロードの場合、Azure やその他のパブリッククラウド環境における単一障害点を回避できます。

DNS セキュリティと制御が強化

近年におけるインターネットサービスプロバイダーの Dyn やその他の組織に対する分散型サービス拒否 (DDoS) 攻撃は、コストがかさむ業務中断、逸失収益、ブランドイメージの低下を最小限に抑えるために、DNS ベースの脅威に対する保護の必要性を浮き彫りにしました。NIOS は、AWS パブリッククラウドに仮想 Advanced DNS Protection (vADP) を追加し、ボリューム攻撃、NXDOMAIN、DNS ハイジャック、その他のエクスプロイトを含む幅広い DNS 攻撃を検出して軽減します。vADP を使用すると、管理者は攻撃を迅速に検出し、DNS の整合性を維持し、稼働時間を向上させ、ローカルのオンプレミスからパブリッククラウド環境まで外部 DNS 保護を拡張できます。

システムのセキュリティをさらに強化するために、Infoblox では Amazon Route 53 マルチアカウントサブセットリストとの vNIOS 同期が有効です。管理者は、1) NIOS が自動的にアカウントを検出するか、2) Route 53 環境から検出して同期するアカウントのリストを指定するかを選択できます。この機能は、1) 子アカウントがルートにアクセスするのを防ぎ、2) 代理管理者のアクセスをブロックし、3) すべての組織単位 (OU) アカウントの発見を抑制し、4) Assume-Role 権限アクセスを使用することでセキュリティを強化します。これらのDNSセキュリティ条項は、重要なネットワークサービスを攻撃から保護し、アプリケーションの可用性とパフォーマンスを維持します。 管理者は、単一の NIOS インスタンスから AWS の複数アカウントに対して Route 53 の検出と同期を拡張できます。また、1) NIOS が自動的にアカウントを検出するか、2) Route 53 環境から検出して同期するアカウントのリストを指定するかを選択できます。この機能は、1) 子アカウントがルートにアクセスするのを防ぎ、2) 代理管理者のアクセスをブロックし、3) すべての組織単位 (OU) アカウントの発見を抑制し、4) Assume-Role 権限アクセスを使用することでセキュリティを強化します。これらの DNS セキュリティ条項は、重要なネットワークサービスを攻撃から保護し、アプリケーションの可用性とパフォーマンスを維持します。

ハイブリッドクラウド向けに一貫した DDI プラットフォームを維持

多くの組織は、オンプレミス、仮想プライベート、ハイブリッド、パブリック、AWS を含むマルチクラウドインフラストラクチャを組み合わせたハイブリッド環境を導入しています。手動の古いスプレッドシートや異なるソリューションの複雑さの代わりに、Infoblox は汎用 DNS サーバーを立ち上げる必要性を軽減し、オンプレミスから AWS への通信を可能にし、複数のプラットフォームにわたる DNS レコードを単一のコントロールプレーンで統合して、一貫性と管理性を向上させます。

InfobloxはEC2 R6インスタンスタイプもサポートしており、パフォーマンスを向上させつつ、総所有コストを削減します。InfobloxはAWS Nitro SystemsとEC2 Serial Consoleへの直接接続を可能にし、より迅速なトラブルシューティングを実現し、ユーザー体験と制御を向上させます。vNIOSは、データの静止時、転送中、およびすべてのボリュームバックアップに対するElastic Block Store（EBS）暗号化を可能にすることで、クラウドのセキュリティと制御をさらに強化します。

柔軟な展開オプション

Infoblox DDI for AWS は、業界をリードするオンプレミス仮想および物理アプライアンスと緊密に統合されています。包括的な DDI プラットフォームは、AWS パブリッククラウド、プライベートクラウド環境 (VMware、OpenStack、Microsoft など)、従来のネットワーク、またはハイブリッド展開における任意の組み合わせをサポートできます。この統合ソリューションにより、最大限の柔軟性、拡張性、およびサービスの可用性が保証されます。

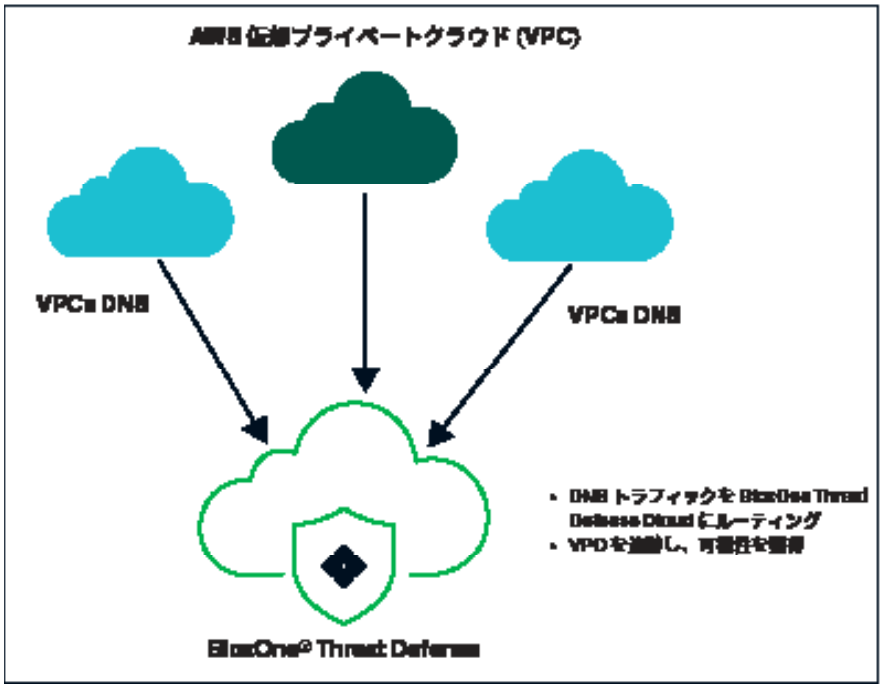
Infoblox は、小規模なリモートオフィスやブランチオフィス、中規模組織、大企業、データセンターや分散サイトを持つサービスプロバイダー向けに、安全な専用の物理アプライアンスとソフトウェアアプライアンスを通じて、幅広い導入オプションを提供します。Trinzic X6 物理的およびソフトウェアのアプライアンスプラットフォームでは、以前のモデルに比べて DNS および DHCP のパフォーマンスが最大 50% 向上します。また、Cloud Platform API 自動化、DNS ファイアウォール、DNS トラフィック制御のグローバルサーバー負荷分散のためのコスト削減ライセンスも含まれています。組織のニーズが何であれ、Infoblox は商業、企業、およびサービスプロバイダー向けのソリューションを提供し、信頼性と柔軟性を備えた一貫した基幹ネットワーク体験を実現します。また、ビジネスの要件に応じて環境をスケールさせることが可能です。

Infoblox は、管理者が AWS パブリッククラウドに Network Insight 検出およびレポート、分析のアプライアンスを展開できるようにすることで、クラウド移行を実現します。Network Insight は、統合されたレイヤー 2 およびレイヤー 3 の検出、デバイス、エンドホスト、ネットワークポートとの IPAM同期、スイッチポート管理、ライフサイクルとコンプライアンスの通知を提供します。さらに、データ検索市場のリーダーである Splunk を基盤とした Infoblox のレポート作成および分析ソリューションは、監視、可視化、SIEM の機能を提供します。AWS にソリューション最適化アプライアンスを配置することで、クラウドファーストの取り組みを支援し、物理データセンターのクラウドへの移行を簡素化し、物理データセンターのリソースを削減します。また、過去の監査やコンプライアンス、リアルタイムアラート、ネットワークパフォーマンス、キャパシティプランニングの DDI メタデータを単一および複数サイトで可視化できます。その結果、組織は完全なオンデマンドでの可視性を得て、コンプライアンス報告を簡素化し、ネットワークや地理的地域全体の AWS リソースの DNS および IPアドレス情報の詳細な監査を実施できます。

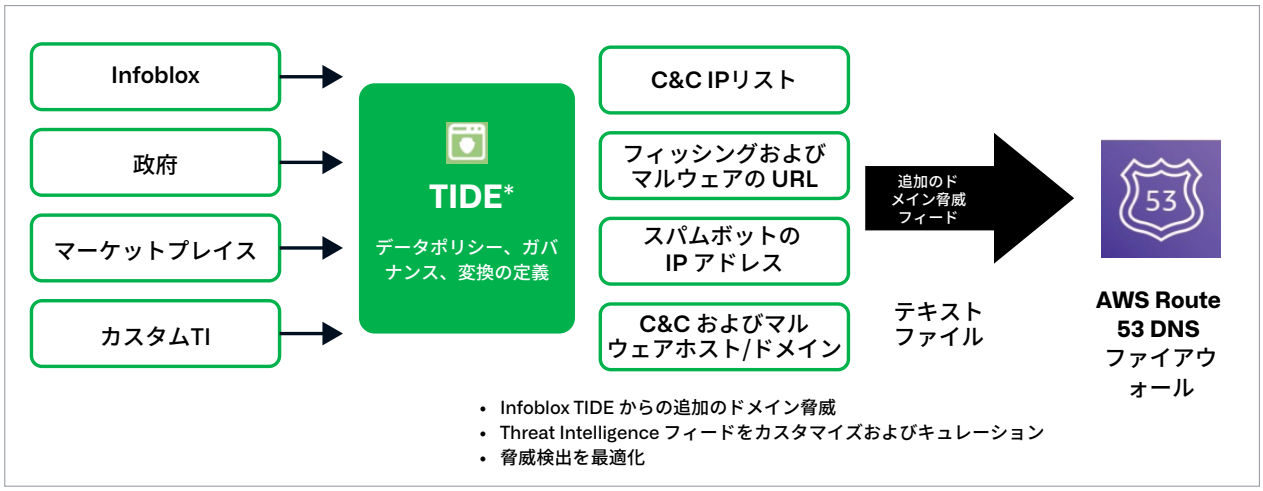
DNSレイヤーセキュリティと脅威検出をAWSに拡張

ユーザーは、Infoblox DNS セキュリティ、IPAM (IPアドレス管理)、厳選された脅威インテリジェンスを活用して、AWS VPC に対する可視性を確保し、Amazon Route 53 DNS ファイアウォールの脅威検出を最適化することもできます。包括的な戦略の一環として Infoblox の BloxOne® Threat Defense を実装することで、高度な攻撃やエクスプロイト、DNS データ流出のリスクを大幅に軽減できます。

広範なエコシステム統合を通じて、ユーザーは検出されたイベントへの対応を自動化し、ネットワークコンテキストを使用して対応の優先順位を付けることができます。ユーザーは、VPC DNS トラフィックを BloxOne Threat Defense Cloud にルーティングし、クラウドインスタンスを追跡して可視化し、サイバー脅威によるリスクを軽減することで、AWS VPC 内の脅威を効果的に管理し、最小限に抑えることができます。



さらに、組織は Infoblox TIDE (Threat Intel Data Exchange プラットフォーム) を活用して、Infoblox の AWS 上の DNS アプライアンスと Amazon Route 53 DNS Firewall の両方に侵害の兆候 (IOC) をプッシュできます。これにより、すべての環境に一貫したセキュリティを適用し、特定のニーズに基づいて選択した脅威インテリジェンスフィードで精度を高めることができます。Infoblox TIDE からの多数の追加脅威フィードにアクセスすることで、Route 53 DNS Firewall によるセキュリティを補強できます。カスタマイズされた「スーパーフィード」による現在の脅威の検出・ブロック機能はセキュリティスタックを強化し、調査、応答能力を向上させます。



結論

Amazon Route 53 は AWS に特化しているため、オンプレミスおよびハイブリッドのマルチクラウドインフラストラクチャを管理する際に、管理とコアネットワークサービスにギャップが生じ、プラットフォーム全体の可視性、一貫性、セキュリティが欠如しています。Infoblox DDI for AWS はこうしたギャップを解消するために、業界をリードする DDI プラットフォームを活用すると同時に、オンプレミス、AWS パブリッククラウド、重要な DNS コンポーネントを単一のコンソールで管理して複雑さを軽減します。BloxOne Threat Defense は DNS のセキュリティ基盤として、脅威検出、応答、エコシステムの統合でハイブリッド環境を保護し、セキュリティパフォーマンスを最適化します。

お問い合わせ

Infoblox の DNS や IPAM、および Amazon Web Services (AWS) 向けのその他のネットワークサービスに関する詳細情報や回答については、Infoblox アカウントチームにお問い合わせいただくか、重要なネットワーク統合を参照するか、Infoblox.com までお問い合わせください。

Infobloxはネットワークとセキュリティを統合して、これまでにないパフォーマンスと保護を提供します。Fortune 100企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に検知・対処できます。

Infoblox株式会社
〒107-0062 東京都港区南青山
2-26-37
VORT外苑前I 3F

03-5772-7211
www.infoblox.com

バージョン: 20240529v2